ICAEW
REPRESENTATION 01/20

DRAFT RIGHT OF ACCESS GUIDANCE

Issued 11 February 2020

ICAEW welcomes the opportunity to comment on the *Draft Right of Access Guidance* published by Information Commissioner's Office (ICO) on 4 December 2019, a copy of which is available from this link.

The right of data subjects to know (and access) what personal data is held by a data controller is a fundamental right of the General Data Protection Regulation (GDPR). It is also beholden upon data controllers to ensure that they respond to a Data Subject Access Request (DSAR) in accordance with the GDPR.

We note, however, that our members have reported to us that the rate of DSARs has increased significantly since the GDPR came into force and this shows no sign of abating. There has also been a rise in the complexity of the requests over the same period, as well as an increase in 'tactical' DSARs, i.e. requests received in the context of an ongoing complaint or grievance and accompanied by the threat of litigation. This has significantly increased the compliance burden on organisations.

Whilst we acknowledge the importance of the right of access, we believe that the Information Commissioner's approach should be pragmatic and proportionate. Organisations have a finite amount of data protection resource and, at present, are having to deploy a large proportion of this to the processing of DSARs; to the detriment of other important areas of data protection compliance.

This ICAEW response of 11 February 2020 reflects consultation with the Business Law Committee and its Data Protection Working Party, both of which include representatives from public practice and the business community. The Committee is responsible for ICAEW policy on business law issues and related submissions to legislators, regulators and other external bodies.

ICAEW is a world-leading professional body established under a Royal Charter to serve the public interest. In pursuit of its vision of a world of strong economies, ICAEW works with governments, regulators and businesses and it leads, connects, supports and regulates more than 150,000 chartered accountant members in over 160 countries. ICAEW members work in all types of private and public organisations, including public practice firms, and are trained to provide clarity and rigour and apply the highest professional, technical and ethical standards.

ICAEW Chartered Accountants' Hall Moorgate Place London EC2R 6EA UK
T +44 (0)20 7920 8100 **icaew.com**

GENERAL POINTS

1. Responding to Data Subject Access Reports (DSARs) is increasingly placing a significant burden on business, and, since the implementation of the GDPR, our members have reported that the number of DSARS received has increased significantly. Some of our members are reporting a three and fourfold increase. The ICO's publication of guidance is therefore welcome and timely.
2. As a general observation, we believe the guidance would benefit from the inclusion of more practical examples, especially around when exemptions may apply, such as that for management planning, or for auditors and insolvency practitioners. The right of access to personal data has existed in UK law for many years now and we expect that the ICO has a large body of 'case law' from which to draw. We note the ICO's guidance on "Access to information held in complaint files", which illustrates the points made on concepts such as 'mixed personal data' with detailed, real life examples[1]. We suggest that this guidance should be cross-referred to (e.g., via a link) in the 'Right of Access' guidance and similar examples be included throughout.
3. Our members have observed that some data subjects have an unrealistic expectation of what information they are entitled to receive and therefore are unhappy with how the DSAR is responded to by the data controller. We believe it would be helpful if the ICO provided more detailed information to data subjects on what they will receive, clearly explaining that it will be limited solely to their own personal data, that various exemptions may apply and that the data controller is entitled to redact business information and the personal data of others. It would also help if the final version of the ICO's guidance on Right of Access included a cross reference or link to the ICO's guidance to data subjects on their rights so that the data controller could point the data subject to this if the latter is unhappy with the response of the data controller
4. There is evidence to suggest that many DSARs are not about individuals seeking to exercise data protection rights, (e.g., checking accuracy, seeking rectification or erasure, or to prevent the unwanted receipt of direct marketing), but are in fact a prelude to employment claims or grievance procedures. Such DSARs can be incredibly onerous, particularly for long standing employees, as it is often necessary to review large quantities of emails and other unstructured data to ensure client information and others' personal data is protected through redaction. There is clearly a continuum between when a request might be considered reasonable and appropriate, when a request is "complex" and when it might be "manifestly unfounded" or "excessive". Additional guidance, backed by illustrative examples, to determine how requests might fall into each category would be beneficial.
5. Whilst not of immediate relevance to the ICO's Right of Access guidance, we recall that under the Data Protection Act 1998 a nominal fee of £10 was allowed. We would suggest that when finalising the UK GDPR serious consideration be given to re-introducing the right for a controller to charge a nominal fee. The intention of such a nominal fee would be not to compensate controllers for their costs, but rather to help restrict DSAR submissions only to those data subjects who have a serious interest in understanding how their personal data is processed.

SPECIFIC POINTS

6. Social Media (page 10)

   The draft guidance on page 10 suggests that data subjects are entitled to make a DSAR using any form of social media site where an organisation has a presence. We think this places an unnecessary burden on smaller businesses who may well have a site on Facebook or Twitter, for example, but as the purpose is to inform clients or potential clients of their services or changes in the law it is not monitored on a regular basis. We would suggest that the guidance makes clear that this only applies if there is an interactive social

[1] https://ico.org.uk/media/1179/access_to_information_held_in_complaint_files.pdf

media presence (i.e., where customers or clients are invited to post their comments) rather than on an unmonitored broadcasting mechanism. Examples of relevant social media sites would also be useful, rather than simply saying all forms of social media can be used to make a DSARs.

7. Time Limits for responding to DSARs (pages16-17)

   The draft guidance seems to suggest that the time limit for a response cannot be paused while the organisation waits for the individual to clarify the request. This approach does not serve either party. We do not believe it is practical for an organisation to simply start searching for any and all information that it might hold about the data subject. This tends to result in extensive search efforts, the results of which take additional time to review and redact. This does not benefit the individual, who has to wait longer for a response, which is likely to contain a large amount of irrelevant data and is an inefficient use of the organisation's own time and resource. The example given on page 24 of the draft guidance of the supermarket customer/employee illustrates exactly this point.

8. Multiple Requests (page 18)

   We would suggest that multiple requests received at the same time – and not simply from the same individual – should also be regarded as 'complex', e.g., an influx of requests received subsequent to the announcement of a proposed restructuring in a business. We note that the ICO already views volume as a relevant factor when considering a complaint[2] and suggest that it is also a relevant factor when assessing complexity

9. Fee (pages 18-19)

   The draft guidance states that it is not possible for an organisation to include a charge for time taken as part of the administrative costs incurred when fulfilling an unfounded/excessive or repeat request. We believe that administrative costs should include time costs as well as photocopying, printing or postage expenses. The exclusion of reasonable time costs from any administrative fee will act to the disadvantage of the data subject as data controllers may choose the option to refuse to act on the request.

10. Identity Checks (pages 19 to 21)

    We suggest that more detailed guidance (to include examples) on checking the identity of the requestor be included, as we are aware that there is evidence to suggest that organisations are being tripped up by the basics.[3] This would also assist in managing the expectations of data subjects regarding the checks an organisation will need to perform to establish their identity, before giving them access to their personal data. We note that Recital 64 of GDPR requires controllers to take 'all reasonable measures' to verify identity. Guidance on what is considered 'reasonable ' in this context would be helpful.

11. Scope of Request (page 23)

    The draft guidance on page 23 states that the data controller cannot ask the data subject "to narrow the scope of their request". It may be a matter of clarifying the language, but as written appears at odds with the preceding paragraph and to contradict Recital 63 of the GDPR which states:

    > 'Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.'

12. Systems (page 23)

    We note the Information Commissioner's view that systems should be designed to allow the redaction of third-party data where necessary. We think it is important that the ICO recognise that, in a large percentage of DSARs, it is not simply a matter of introducing a new system or element of automation. Many DSARs are received from an organisation's own staff members

[2] P22, 'in considering a complaint about a DSAR, the ICO will have regard to the volume of requests received by an organisation and the steps they have taken to ensure requests are dealt with appropriately even when facing a high volume of similar requests.'

[3] https://www.bbc.com/news/technology-49252501 *Black Hat: GDPR privacy law exploited to reveal personal data*

and are seeking email correspondence and other documentation that contains a mixture of personal and other, company related, information. It must be carefully reviewed to (i) extract the requestor's own personal data from the surrounding information; and (ii) where data is 'mixed', balance the competing rights of third-party data subjects against those of the requestor. This requires specialist data protection expertise and a high degree of subjective judgement and we know of no technology currently available to allow this

13. Appropriate record management procedures (page 24)

    On page 24 the draft guidance states that organisations need to have 'appropriate record management procedures in place to handle large requests and locate information efficiently.' We are understand that for many organisations the sheer volume of legacy/historical data means it will take time for them to be able to retrieve data and therefore this needs to be taken into account when handling of multiple requests (see also point 8 above). We think it would be helpful if the guidance from the ICO suggested that in such situations it is appropriate for an organisation to keep the data subject aware and updated as to the retrieval process if this is going to take some time.

14. Emails (page 26)

    We note that the draft guidance is relatively thin on how to deal with unstructured data such as emails. As discussed above, the identification and review of emails, together with the redaction of unnecessary information can be particularly onerous in practice. Additional guidance and examples on what searches are considered reasonable, particularly in the absence of additional context from the data subject, would be helpful.

15. Relevant Data (page 29 and page 33)

    The guidance on page 29 (last paragraph) and on page 33 seem contradictory. On page 29 the guidance states that a data controller can give the 'requester a mixture of all the personal data and ordinary information relevant to their request, rather than to look at every document'. On page 33, however, the draft guidance states that the information should not include any 'that is irrelevant or unnecessary'. In practice, it is difficult to extract sensitive or others' personal data or assess whether it is relevant or necessary without looking at every document in detail. Further clarification on this point be would helpful.

ANSWERS TO THE CONSULTATION QUESTIONS

Q1 Does the draft guidance cover the relevant issues about the right of access?

☒ Yes

☐ No

☐ Unsure/don't know

If no or unsure/don't know, what other issues would you like to be covered in it?

N/A

Q2 Does the draft guidance contain the right level of detail?

☐ Yes

☒ No

☐ Unsure/don't know

If no or unsure/don't know, in what areas should there be more detail within the draft guidance?

Although there the guidance is very detailed but as noted above (see our Specific Points) there are a number of areas where we feel more detail would be helpful. See also our answer to Q6 below.

Q3 Does the draft guidance contain enough examples?

☐ Yes

☒ No

☐ Unsure/don't know

If no or unsure/don't know, please provide any examples that you think should be included in the draft guidance

We would welcome more examples in general and in particular examples that relate to the accountancy sector. We would be happy to provide such examples. See also points 2, 4, 6 and 10 above

Q4 We have found that data protection professionals often struggle with applying and defining 'manifestly unfounded or excessive' subject access requests. We would like to include a wide range of examples from a variety of sectors to help you. Please provide some examples of manifestly unfounded and excessive requests below (if applicable).

1. In employment disputes – see point 4 above 2. Membership organisations – when members wish to leave the organisation they frequently request all the personal data held on them and ask this to include all the emails they have received from the organisation. These may include emails about events, news, updates which although generic will be addressed to them personally. 3. In grievance cases - where employees are simply making DSAR's to see what is being said about them (and see point 4 above) 4. Prior to litigation – a DSARs may simply be a 'fishing' expedition as all data will be requested (and see point 4 above).

Q5 On a scale of 1-5 how useful is the draft guidance?

1 – Not at all useful	2 – Slightly useful	3 – Moderately useful	4 – Very useful	5 – Extremely useful
☐	☐	☐	☒	☐

Q6 Why have you given this score?

For many of our members responding to DSARs is the most time-consuming activity they have to undertake in order to remain compliance with the GDPR and Data Protection Act 2018, so any additional guidance is welcome.
More examples and the removal of a number of apparent contradictions as outlined in our comments above would, however, make the guidance more useful.
The guidance is aimed at data controllers and as pointed out above we feel it would also be useful to give more detailed specific and separate guidance to data subjects and to cross refer to this in the guidance for data controllers so that they may share this with or point the data subject to this. This would help all parties involved to understand the process and the outcome of any request (see also point 3 above).

Q7 To what extent do you agree that the draft guidance is clear and easy to understand?

Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
☐	☐	☒	☐	☐

Q8 Please provide any further comments or suggestions you may have about the draft guidance.

The guidance states that it is written for experienced data protection officers or others with responsibility for data protection in larger organisations and it is clear that it assumes a familiarity with the terms and the legislation. This means it may be of limited use to those new to the DPA 2018 and GDPR regime or for those who work for smaller orgqanisations. Our members have confirned that smaller organisations are also experiencing an increased number of DSARs and such organisations may not possess sufficient detailed knowledge or have the resources to deal with them as appropriate.
We think it may be more helpful to include a brief summary (as you do in the Draft Direct Marketing Code of Practice) and a glossary of terms rather than directing people to the 'in brief' guide.

Q9 Are you answering as:

- ☐ An individual acting in a private capacity (**e.g.,** someone providing their views as a member of the public)
- ☐ An individual acting in a professional capacity
- ☒ On behalf of an organisation
- ☐ Other

Please specify the name of your organisation:

ICAEW

What sector are you from?

Professional Services - Accountancy

Q10 How did you find out about this survey?

- ☐ ICO Twitter account
- ☐ ICO Facebook account
- ☐ ICO LinkedIn account
- ☐ ICO website
- ☒ ICO newsletter
- ☐ ICO staff member
- ☐ Colleague
- ☐ Personal/work Twitter account
- ☐ Personal/work Facebook account
- ☐ Personal/work LinkedIn account
- ☐ Other